مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

TLS Vulnerability in CrowdStrike Falcon Sensor for Linux

Tracking #:432316862

Date:13-02-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed CrowdStrike has disclosed a high-severity vulnerability in its Falcon Sensor for Linux, Falcon Kubernetes Admission Controller, and Falcon Container Sensor.

TECHNICAL DETAILS:

CrowdStrike has disclosed a high-severity vulnerability (CVE-2025-1146) in its Falcon Sensor for Linux, Falcon Kubernetes Admission Controller, and Falcon Container Sensor. This vulnerability stems from a Transport Layer Security (TLS) validation logic error, potentially allowing attackers to carry out man-in-the-middle (MiTM) attacks, intercepting and manipulating communication between the affected sensor software and the CrowdStrike cloud.

Vulnerability Details:

- **CVE ID:** CVE-2025-1146
- **Vulnerability Type:** TLS Validation Logic Error
- **Severity Rating:** High (CVSS v3.1 score of 8.1)
- **Impact:**
  - Potential for Man-in-the-Middle (MiTM) attacks
  - Interception and manipulation of traffic between the Falcon Sensor and the CrowdStrike cloud
  - Compromise of confidentiality and integrity of sensitive data transmitted between the sensor and cloud
- **Affected Products:**
  - Falcon Sensor for Linux (all versions prior to 7.21)
  - Falcon Kubernetes Admission Controller (all versions prior to 7.21)
  - Falcon Container Sensor (all versions prior to 7.21)
- **Mitigation:**
  - CrowdStrike has addressed the vulnerability in version 7.21 of the affected products.

RECOMMENDATIONS:

- Update all instances of Falcon Sensor for Linux, Falcon Kubernetes Admission Controller, and Falcon Container Sensor to fixed version or apply the available hotfixes for supported and unsupported sensor versions via the Falcon console or binary downloads.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.crowdstrike.com/security-advisories/cve-2025-1146